REMARKS

This is in full and timely response to the above-identified Office Action. The above listing of the claims supersedes any previous listing. Favorable reexamination and reconsideration are respectfully requested in view of the preceding amendments and the following remarks.

Claim amendments/Status

In this response, the claims have been reviewed and amendments made which overcome the rejections made under 35 USC § 112, second paragraph. That is to say, the antecedent basis problems with "the signal" and "the fuse", have been corrected, "not valid" has been changed to "invalid" and the inadvertent mistyping of "KO" has been changed to "OK" where appropriate.

Claims 1-9 remain pending in the application.

Rejections under 35 USC § 102

The rejection of claims 1-9 under 35 USC 102(b) as being anticipated by Sormunen et al. (US Patent Pub. No. US 2003/0014663) is respectfully traversed.

The claimed subject matter is directed to a method making it possible to detect and/or to avoid the modification of software embedded in a programmable memory within a system wherein a hard kernel containing hardware security functions suitable for verifying the integrity of a soft kernel comprising a programmable memory, the system comprising a local data interface, characterized in that it comprises at least the following steps:

A1 — the signal received on the local data interface is not valid, place the system in a disabled state,

B1 — the signal received on the local data interface is a disconnection signal, or there is no signal, instigate a secure startup procedure, with execution of the control functions:

Autotest of the hard kernel:

- If the autotest is OK, then test the integrity of the reprogrammable memory,
  - If this integrity is OK, then activate the system for normal operation
  - If this integrity is OK, then place the system in a disabled state

- If the autotest is OK, then place the system in a disabled state,

CI — the received signal is a valid startup signal,

- If the system is in a development mode, render it enabled,

- If the system is in an enabled utilization mode and if the signal is a test signal, then deactivate at least one of the essential functions of enabled operation.

- Another characteristic of the method according to the invention is that the exchange of the data between the hard kernel and the soft kernel is performed by using an algorithm based on the principle of non-replay and of nonpredictability of the transmitted data.

Prior art cited by the Examiner

The patent application US 2003/0014663 to Sormunen concerns a method for securing an electronic device. Paragraph [0014] of this reference discloses that the disclosed invention is directed to an improved method for securing an electronic device in such a way that a given program is set to function in a given electronic device only. To obtain this result, the invention is based on the fact that the boot-up is set to consist of at least two steps in such a way that in the first step, first check-up data is verified, and if the first-check-up data is correct, second check-up data related to the second booting step is verified, wherein if also the second check-up data is correct, it is possible to start the second booting step. However, if the second check-up data is not correct, then, the device is put on a disable state.

Paragraph [0031] states that the device can be a GSM or UMTS device. Paragraphs [0032] and following passages, mention the data that can be checked by the method according to the invention.

In [0033] the initial booting is executed according a prior art method. During this initial step, the identity ID of the device is checked. The checking is performed by computing a digital signature by using at least said device identity DID. Moreover, it is possible to check that the program code corresponding to the first block P1 relating to the first step of booting has not been changed.

Generally, for checking of data, the method in this patent application to Sormunen uses signature checking. If the signatures match one another, then, the method considers that there is no modification of the program of the electronic device to be protected.

The checking is preferably performed in the control block 2 by computing a digital signature by using at least said device identity DID and (possibly) also at least part of the boot program stored in the read-only memory 2d, 2 e.

In the computing of the digital signature, the same algorithm and the same data are used, by which the digital signature was computed in connection with the manufacture of the electronic device 1 using a secret key of the device manufacturer, as will be discussed below. This digital signature is preferably stored in the programmable read-only memory 3b (indicated with reference 51 in FI.2). However, it is obvious that it can be also be stored, for example, in the same read-only memory 2d, 2 e, in which the device identity DID has been stored.

The digital signature can be verified by using the public

key PK1 which corresponds to the secret key used in the signature and is stored in the read-only memory 2d, 2 e. After the computing of the digital signature, a comparison is made between the digital signature computed in the control block 2 and the digital signature S1 stored in the one time programmable read-only memory 2d, 2 e, block (503).

If the comparison shows that the digital signatures match, it is possible to continue the booting. In other cases, it is obvious that an attempt has been made to modify the electronic device 1 and/or the identity data DID contained in it and/or the boot program, wherein as a result, the normal operation of the device is prevented, for example by switching off the electronic device (block 504). Viz., the device is put into a disabled state.

If the first step is valid, i.e. the first checking of data is OK, and the data have not been modified, then the second step consists of:

« In the second check-up step, the authenticity of the second boot block P2 of the boot program is checked. The second boot block P2 of the boot program is preferably stored in the electrically erasable programmable read only memory (EEPROM) 3b, such as a Flash Memory. A digital signature is computed by using at least part of the boot program stored in the read-only memory 3a, 3b (block 505). Also the digital signature S2 of the second boot block of the boot program is stored in the same memory 3b. The computation of this digital signature S2 applies some data that can be verified, such as a part of the program code of the second boot block of the boot program as well as the secret key of the manufacturer of the electronic device 1.

The public key PK2 corresponding to this secret key is also stored in the memory 3b. The computed digital signature is compared with the digital signature stored in the memory 3b (block 506), and if the signatures match, the booting of the electronic device 1 can be continued further. However if the signatures do not match, the normal operation of the device is prevented, for example, by halting the operation of the electronic device.

This second step is always based on a signature checking.

The data to be checked (second check-up data, second security data) in the second check-up step may have been formed, for example, by computing compressed data H, e.g. by a hash function, from programs PG1, PG2, PG3, parameters, device identities DID, IMEI, or the like, stored in the programmable read-only memory 3b.

In this case, the checking is performed by verifying the authenticity of this signature.

In conclusion, the US patent application to Sormunen fails to disclose the use of a signal on the data interface, and its checking, such as described, for example, on page 7 line 10 "Reception of a signal at the level of the local data interface of the GSM terminal: activation of the SPLIT function (inhibiting of an essential function rendering the terminal disabled)" of the Thales patent application and as recited in the claim 1.

To check said signal, allows anticipating an illicit intrusion. This feature is not mentioned in the Somunen patent. The object in Somunen is to verify that a given program is set to function in a given electronic device only. The Applicant's position is that the teaching of Somunen fails to disclose or suggest the ability of avoiding illicit intrusion by checking a signal, not directly in the device, but by the signal on the interface of the device.

With the device of Somunen it is not possible to avoid intrusion, because, checking is realized inside the device, in order to check that a given program is set to function in a given electronic device only.

That is why the data checking uses signatures verification and that's why the Sormunen document fails to teach using a signal on the data interface and why the anticipation rejection is deemed untenable.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

The Examiner is invited to telephone the undersigned, Applicant's attorney of record, to facilitate advancement of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,
LOWE HAUPTMAN HAM & BERNER, LLP

Kenneth M. Berner

Kenneth M. Berner
Registration No. 37,093

1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: February 18, 2009
KMB/KJT/cac